Teorija izračunljivosti

Ivan Prokić
kabinet 117, F blok
prokic@uns.ac.rs
http://imft.ftn.uns.ac.rs/∼iprokic/

Novi Sad

Tema 1

Univerzalna Tjuringova mašina U

Univerzalna Tjuringova mašina

- Tjuring je dao opis, naziv u origilnalu: ”Universal Computing Machine”;
- Ovo je prvi primer mašine koja je mogla da se programira, bez potrebe da se hardver mašine modifikuje za svaki novi program;
- Univerzalna mašina radi po instrukcijama, koje se u suštini ne razlikuju od ulaznih podataka
- Univerzalna Tjuringova mašina je bila inspitacija fon Nojmanovu da osmisli njegovu čuvenu arhitekturu računara.

Univerzalna Tjuringova mašina U

- Po Čerč-Tjurinovoj tezi svaki algoritam možemo identifikovati sa jednom Tjuringovom mašinom (koja taj algoritam izvršava);
- Tjuring je primetio da svaku Tjuringovu mašinu možemo kodirati kao ulazni podatak (tj. program);
- Univerzalna Tjuringova mašina U izvršava **svaki program**;

Univerzalna Tjuringova mašina

Osnovna ideja univerzalne Tjurnove mašine:

- prvo, sve Tjuringove mašine i sve reči koje one prihvataju kodiramo (na neki način) sa

$$<M, w>$$

  tako da kod pripada (nekoj) fiksnoj azbuci Univerzalne mašine Σ_U;
- taj kod koristimo kao ulazne podatke Univerzalne mašine;
- odnosno, treba nam da jezik Univerzanle mašine bude

$$L(U) = \{<M, w> \mid w \in L(M)\}$$

  tj. da U prihvata $<M, w>$ ako i samo ako M prihvata w.

Jedno kodiranje

- Kodiranje ćemo napraviti tako da azbuka mašine U bude $L_U = \{0, 1, \#\}$.
- Setimo se da svaki jezik možemo kodirati kao podskup skupa prirodnih brojeva (vidi deo sa rekurzivnim skupovima i jezicima);
- Zato, bez umanjenja opštosti, pretpostavimo da za svaku Tjuringovu mašinu $M = (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ važi:
  1. skup stanja $Q = \{0, \ldots, n-1\}$;
  2. ulazna azbuka $\Sigma = \{0, \ldots, m-1\}$;
  3. azbuka trake $\Gamma = \{0, \ldots, m-1, \ldots, k-1\}$;

  pri čemu $s, a, r \in Q$ su redom stanja početno, prihvatanja i odbijanja i $b \in \Gamma \backslash \Sigma$ je simbol blanko.
- Početak koda mašine M bi mogao biti

$$0^n 1 0^m 1 0^k 1 0^s 1 0^a 1 0^r 1 0^b 1$$

Kod se lako dekodira: M ima n stanja (od kojih su s, a, r su početno, prihvatanja i odbijanja), k simbola (od kojih je m ulaznih i b je simbol blanko).

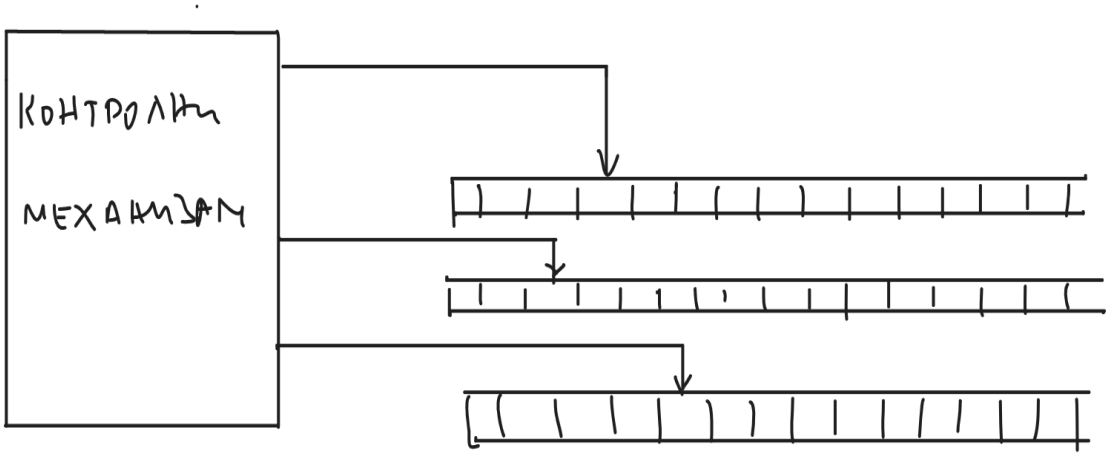
Jedno kodiranje: nastavak

- kodiranje funkcije prelaza:
  1. za svako $\delta(q, a) = (p, b, L)$ kod je
  $$0^q 1 0^a 1 0^p 1 0^b 1 0 1,$$
  2. za svako $\delta(q, a) = (p, b, R)$ kod je
  $$0^q 1 0^a 1 0^p 1 0^b 1 0 0 1;$$
- kodiranje reči $w = a_1 \dots a_i$ je
$$<w> = 0^{a_1} 1 \dots 1 0^{a_i},$$
i $<\lambda> = \lambda$ (kod od prazne reči je prazna reč).
- Na kraju, definišemo
$$<M, w> = <M>\#<w>.$$

Univerzalna Tjuringova mašina: skica

Univerzalna mašina U ima tri trake. Na početku:

- Na prvoj traci je kod ulaznih podataka, u obliku $<M>\#<w>$;
- Druga i treća traka su prazne.



Univerzalna Tjuringova mašina: početak rada

- **Priprema**: Na početku, mašina U vrši proveru da li sadržaj prve trake odgovara kodu neke Tjuringove mašine i reči nad njenom azbukom, tj. da li na traci piše $<M>\#<w>$, za neku Tjuringovu mašinu M i reč w nad ulaznom azbukom mašine M. Ako to nije ispunjeno U prelazi u stanje odbijanja.
- **Početak**: Ako na prvoj traci zaista piše $<M>\#<w>$, mašina U:
  1. na drugu traku prepisuje $<w>$, tj. kod početnog sadržaja trake mašine M, i glavu postavi na početak trake;
  2. na treću prepisuje 0^s, tj. kod početnog stanja mašine M;

Univerzalna Tjuringova mašina: jedan korak u radu

Simulacija: U simulira rad mašine M za ulaz w na sledeći način:

- Sa druge trake pročita niz nula (koji predstavlja kod simbola a) na čiji početak glava trenutno pokazuje;
- Sa treće trake pročita kod trenutnog stanja kontrolnog mehanizma (q) mašine M;
- Za pročitane q i a, na prvoj traci u kodu funkcije prelaza mašine M pronađe kod od $\delta(q, a)$. Ako je, recimo, $\delta(q, a) = (p, b, L)$, taj niz je oblika
$$0^q 1 0^a 1 0^p 1 0^b 1 0 1;$$
- Sada, na drugoj traci briše niz nula (kod simbola a), upisuje kod simbola b i glava se pomera na niz nula sa leve strane;
- Sa treće trake briše kod stanja q i upisuje kod stanja p, tj. upisuje 0^p.

Ako se na trećoj traci pojavi 0^a (odnosno 0^r), mašina U prelazi u stanje prihvatanja (odnosno odbijanja).

Univerzalna Tjuringova mašina U

Univerzalna Tjurinogva mašina U prihvata/odbija/ulazi u mrtvu petlju za ulaz $<M>\#<w>$

ako i samo ako

Tjuringova mašina M prihvata/odbija/ulazi u mrtvu petlju za ulaz w.

Tema 2

Odlučivost

Klasifikacija jezika

U delu sa rekuzivnim funkcijama i skupovima smo videli da važi

$$\mathbf{PR} \subset \mathbf{R} \subseteq \mathbf{RE} \subseteq P(\mathbb{N}),$$

a sada u delu sa Tjuringovim mašinama da važi

$$\mathbf{R} = \text{Tjuring prepoznatljiv} \qquad \text{i} \qquad \mathbf{RE} = \text{Tjuring odlučiv.}$$

Sada ćemo pokazati:

- $\mathbf{RE} \subset P(\mathbb{N})$, tj. da postoje jezici koji nisu rekurzivno nabrojivi, odnosno Tjuring prepoznatljivi i
- $\mathbf{R} \subseteq \mathbf{RE}$, tj. da postoje jezici koji su rekurzivno nabrojivi a nisu rekurzivni, odnosno jezici koji su Tjuring prepoznatljivi a nisu Tjuring odlučivi.

Jezici koji nisu rekurzivno nabrojivi

Podsećanje: reči su konačni nizovi simbola.

Lema

Skup svih reči nad azbukom $\Sigma = \{0, 1\}$ je prebrojiv, tj. $|\Sigma^*| = \aleph_0$.

Jasno je da Σ^* ima beskonačno mnogo reči. Definišemo funkciju $f : \Sigma^* \to \mathbb{N}$ sa $f(w) = 1w$, za $w \in \Sigma^*$, gde $1w$ predstavlja prirodan broj u binarnom zapisu (prva cifra je 1 a ostale cifre su određene simbolima reči w). Jasno da za $w \neq w'$ važi $f(w) = 1w \neq 1w' = f(w')$, pa je f injektivna, odakle sledi $|\Sigma^*| \leqslant |\mathbb{N}| = \aleph_0$.

Lema

Tjuringovih mašina ima prebrojivo mnogo.

Videli smo da se svaka Tjuringova mašina može kodirati kao konačan niz nula i jedinica, tj. $<M> \in \Sigma^*$, za $\Sigma = \{0, 1\}$. Iz prethodne leme sledi da Tjuringovih mašina ima ne više od $\aleph_0$.

Jezici koji nisu rekurzivno nabrojivi

Lema

Neka je B skup svih beskonačnih nizova nula i jedinica, tj. $B = \{f \mid f : \mathbb{N} \to \{0,1\}\}$. Skup B je neprebrojiv, odnosno $|B| = \mathfrak{c}$.

Dokaz izvodimo Kantorovim postupkom dijagonalizacije. Pretpostavimo suprotno: da je B prebrojiv, tj. da je $B = \{a_0, a_1, a_2, \ldots\}$, i neka su

$$\begin{array}{lcl} a_0 & = & \underline{0}101010101\ldots \\ a_1 & = & 0\underline{1}01000111\ldots \\ a_2 & = & 11\underline{1}1011101\ldots \\ \vdots & & \vdots \end{array}$$

Ako sada uzmemo $a \in B$ takvo da se od a_0 razlikuje u prvoj cifri, od a_1 u drugoj, od a_2 u trećoj, itd, vidimo da je $a \neq a_i$, za sve $i \in \mathbb{N}$. Pošto smo dobili kontradikciju (da $a \notin B$), zaključujemo da je B neprebrojiv.

Jezici koji nisu rekurzivno nabrojivi

Lema

Svih jezika nad $\Sigma = \{0, 1\}$ ima neprebrojivo mnogo.

Neka je $\mathbb{L}$ skup svih jezika nad Σ i B skup svih beskonačnih nizova nad Σ. Definišemo funkciju $f : \mathbb{L} \to B$ sa $f(A) = \phi_A$, za $A \in \mathbb{L}$, gde je ϕ_A karakteristični niz jezika A. Kako je

$$\Sigma^* = \{\lambda, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\},$$

za, na primer, $A = \{1, 11, 001\}$ imali bismo $f(A) = 0010001010000\ldots$ Pošto je f bijekcija, sledi $|\mathbb{L}| = |B|$, pa tvrđenje sledi na osnovu prethodne leme.

Teorema

Postoje jezici koji nisu rekurzivno nabrojivi, tj. Tjuring prepoznatljivi.

Pošto Tjuringovih mašina ima prebrojivo mnogo, a svakoj Tjuringovoj mašini odgovara jedan rekurzivno nabrojiv jezik, znamo da i rekurzivno nabrojivih jezika ima prebrojivo mnogo. Pošto svih jezika ima neprebrojivo mnogo, zaključujemo da postoje jezici koji nisu rekurzivno nabrojivi (tj. Tjuring prepoznatljivi).

Rekurzivno nabrojiv jezik

Neka je $L(U)$ jezik univerzalne Tjuringove mašine, tj.

$$L(U) = \{<M, w> \ : \ M \text{ je Tjuringova mašina i } M \text{ prihvata } w\}.$$

Teorema

Jezik $L(U)$ jeste rekurzivno nabrojiv, tj. Tjuring-prepoznatljiv.

Već smo ustanovili da U radi:
$U =$ "Za ulaz $<M, w>$:

1. Simulira rad mašine M za ulaz w;
2. Ako M prihvata w, onda U prelazi u stanje prihvatanja, inače ulazi u mrtvu petlju ili u stanje odbijanja."

Rekurzivno nabrojiv jezik koji nije rekurzivan

Jezik univerzalne Tjuringove odgovara **problemu pripadanja** (eng. membership problem):

Za datu Tjuringovu mašinu M i reč w iz njene azbuke, da li $w \in L(M)$?

Ako bi postojala Tjuringova mašina koja bi odlučivala problem pripadanja, tada bi ona odlučivala sve Tjuring prepoznatljive jezike, tj. važilo bi $\mathbf{R} = \mathbf{RE}$. Sledeća teorema pokazuje da to nije tačno.

Teorema

Jezik $L(U)$ nije rekurzivan, tj. odlučiv.

$L(U)$ nije rekurzivan: dokaz

Dokaz se izvodi svođenjem na kontradikciju i koristi Kantorov postupak dijagonalizacije. Pretpostavimo suprotno: da je $L(U)$ odlučiv. Tada postoji Tjuringova mašina H koja odlučuje $L(U)$:
$H =$ "Za ulaz $<M, w>$:

1. H se zaustavlja i prihvata ako M prihvata w;
2. H se zaustavlja i odbija ako M ne prihvata w."

Sada kostruišemo novu Tjuringovu mašinu D koja koristi H da utvrdi da li M prihvata/odbija/ulazi u mrtvu petlju za ulaz $<M>$. Zatim D radi suprotno od H:
$D =$ "Za ulaz $<M>$, gde je M Tjuringova mašina:

1. Primeni H na $<M, <M>>$ (proverava da li M prihavata reč koja predstavlja njen kod);
2. Izbaci suprotno od H: prihvati ako H odbija, odbij ako H prihvata."

Mašina D radi sledeće:

$$D(<M>) = \begin{cases} \text{prihvata} & \text{, ako } M \text{ ne prihvata } <M> \\ \text{odbija} & \text{, ako } M \text{ prihvata } <M> \end{cases}$$

Ali ako sada za D uzmemo ulaz $<D>$ dobijamo kontradikciju

$$D(<D>) = \begin{cases} \text{prihvata} & \text{, ako } D \text{ ne prihvata } <D> \\ \text{odbija} & \text{, ako } D \text{ prihvata } <D> \end{cases}$$

Dakle, Tjuringove mašine H i D ne postoje.

$L(U)$ nije rekurzivan: dijagonalizacija u dokazu

Neka su $\{M_0, M_1, M_2, \ldots\}$ sve Tjuringove mašine (kojih ima prebrojivo mnogo). Recimo da važi

	$<M_0>$	$<M_1>$	$<M_2>$	$\ldots$
M_0	prihvata		prihvata	$\ldots$
M_1			prihvata	$\ldots$
M_2	prihvata	prihvata	prihvata	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

gde je sa ”prihvata” obeleženo ako M_i prihvata reč $<M_j>$, a ako odbija ili ulazi u mrtvu petlju ostavljeno je prazno polje. Sada H radi kao u sledećoj tabeli (u koju je dodato i D), a D radi suprotno od podvučenih polja na dijagonali. Kontradikcija se pojavljuje kod znaka pitanja.

H	$<M_0>$	$<M_1>$	$<M_2>$	$\ldots$	$<D>$	$\ldots$
M_0	<u>prihvata</u>	odbija	prihvata	$\ldots$	prihvata	$\ldots$
M_1	odbija	<u>odbija</u>	prihvata	$\ldots$	odbija	$\ldots$
M_2	prihvata	prihvata	<u>prihvata</u>	$\ldots$	odbija	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
D	prihvata	odbija	prihvata	$\ldots$	<u>?</u>	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Jedan primer jezika koji nije rekurzivno nabrojiv

Komplement jezika $\overline{L} = \Sigma^* \backslash L$ (sadrži sve reči nad Σ koje nisu u L).

Teorema (Postova - ponovo)

Jezici L i $\overline{L}$ rekurzivno nabrojivi ako i samo ako je L rekurzivan.

($\Rightarrow$): Ako je L rekurzivan, tada je i $\overline{L}$ rekurzivan, a svi rekurzivni jezici su i rekurzivno nabrojivi.
($\Leftarrow$): Neka su L i $\overline{L}$ rekurzivno nabrojivi i neka su M_1 i M_2 Tjuringove mašine takve da $L(M_1) = L$ i $L(M_2) = \overline{L}$. Sada konstrušemo totalnu Tjuringovu mašinu M takvu da $L(M) = L$ (koja odlučuje L):
$M =$ "Za ulaz w:

1. Pokreni M_1 i M_2 paralelno (na dve posebne trake) za ulaz w;
2. Ako M_1 prihvata - prihvati; ako M_2 prihvata - odbaci."

Pošto reč w pripada jeziku L ili $\overline{L}$, tačno jedna od mašina M_1 ili M_2 mora da prihvati reč w.

Posledica

Jezik $\overline{L(U)}$ nije rekurzivno nabrojiv.

Znamo da je $L(U)$ rekurzivno nabrojiv i nije rekurzivan. Ako bi $\overline{L(U)}$ bio rekurzivno nabrojiv, $L(U)$ bi morao biti rekurzivan (po Postovoj teoremi), što je netačno.

Tema 3

Redukcije

Redukcije

Redukcija je izračunljiva funkcija koja jedan problem konvertuje u drugi, na takav način da nam rešenje drugog problema može rešiti i prvi.
Podsetimo se šta su (Tjuring) izračunljive funkcije:

Definicija

Funkcija $f : \Sigma^* \to \Sigma^*$ je **izračunljiva** *ako postoji Tjuringova mašina koja se za svaki ulaz $w \in \Sigma^*$ zaustavlja sa $f(w)$ na traci (pri čemu glava pokazuje na prvo slovo reči $f(w)$).*

Sada definišemo redukcije između jezika:

Definicija

Jezik A se **redukuje** *na jezik B, u oznaci $A \leqslant B$, ako postoji izračunljiva funkcija $f : \Sigma^* \to \Sigma^*$ takva da za svako w važi:*

$$w \in A \quad \Leftrightarrow \quad f(w) \in B.$$

Redukcije

Funkcija f iz prethodne definicije se zove **redukcija**.
Za jezik možemo proveriti da li je rekurzivan (odlučiv) tako što ga svedemo na drugi za koji već znamo da je odlučiv.

Teorema

Ako je $A \leqslant B$ i B je rekurzivan, tada je i A rekurzivan.

Neka je M totalna Tjuringova mašina koja odlučuje B i neka je f redukcija iz A u B (tj. $w \in A \;\Leftrightarrow\; f(w) \in B$). Sada jezik A odlučuje totalna mašina N data sa:
$N =$ "Za ulaz w:

1. Izračunaj $f(w)$;
2. Pokreni mašinu M za ulaz $f(w)$. Ako M prihvata (tj. ako $f(w) \in B$)- prihvati, ako M odbija (tj. ako $f(w) \notin B$) - dobij."

Ista teorema važi i ako umesto "rekurzivan" napišemo "rekurzivno nabrojiv" (tj. Tjuring prepoznatljiv) (dokaz za domaći).

Redukcije

Za dokazivanje da neki jezik nije rekurzivan koristimo posledicu prethodne teoreme:

Posledica

Ako je $A \leqslant B$ i A nije rekurzivan (rekurzivno nabrojiv), tada ni B nije rekurzivan (rekurzivno nabrojiv).

Jedan način da se pokaže da neki jezik nije rekurzivan (odnosno rekurzivno nabrojiv) jeste da jezik $L(U)$ (odnosno jezik $\overline{L(U)}$) redukujemo da taj jezik.

Halting problem

Halting problem (problem zaustavljanja Tjuringove mašine) možemo definisati preko jezika

$$L_{halt} = \{<M, w> \ : \ M \text{ je Tjuringova mašina i } M \text{ se zaustavlja za } w\}.$$

Teorema

L_{halt} nije rekuzivan (tj. nije odlučiv).

Problem pripadanja svodimo na Halting problem. Dokaz izvodimo kontradikcijom. Pretpostavimo da je L_{halt} odlučiv i neka je N totalna Tjuringova mašina koja ga odlučuje. Sada konstruišmo novu Tjuringovu mašinu R sa:
$R =$ "Za ulaz $<M, w>$:

1. pokreni N za ulaz $<M, w>$;
2. ako N odbija - odbij;
3. ako N prihvata, simuliraj rad mašine M za ulaz w: ako M prihvata - prihvati, ako M odbija - odbij."

Dobili smo da R za ulaz $<M, w>$ prihvata ako M prihvata w, a odbija ako M odbija w ili ako upada u mrtvu petlju za w (to je slučaj kada N odbija). Dakle, mašina N odlučuje jezik $L(U)$ - što je kontradikcija jer je $L(U)$ neodlučiv. (Nećemo ulaziti u detalje redukcije f iz $L(U)$ u L_{halt}.)

Još neodlučivih problema

- **Deseti Hilbertov problem**: David Hilbert je 1900. na svetskom kongresu matematičara predstavio 23 otvorena matematička problema za koje je verovao da su najvažnija u tom trenutku. Deseti Hilbertov problem je bio **rešivost diofantskih jednačina**: naći algoritam koji će za svaki polinom sa više promenljivih i celim koeficijentima udvrditi da li ima koren u skupu celih brojeva. Godine 1970. ruski matematičar Jurij Matijaševič je pokazao da je ovaj problem **nedolučiv** jer se Halting problem može svesti na njega.
- **Problem domina**.
- **Postov problem korespondencije**.
- ...